



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/719,812

11/21/2003

Terrence A. Tomkow

RPOST-66232

3326

24201 7590 07/19/2007  
FULWIDER PATTON LLP  
HOWARD HUGHES CENTER  
6060 CENTER DRIVE, TENTH FLOOR  
LOS ANGELES, CA 90045

EXAMINER

HENNING, MATTHEW T

ART UNIT

PAPER NUMBER

2131

MAIL DATE

DELIVERY MODE

07/19/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

CP

<b>Office Action Summary</b>	Application No. 10/719,812	Applicant(s) TOMKOW, TERRENCE A.	
	Examiner Matthew T. Henning	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 November 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-47 is/are pending in the application.  
     4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 and 26-47 is/are rejected.
- 7) ☒ Claim(s) 25 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10 May 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
     a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>10/26/2004</u> . | 6) <input type="checkbox"/> Other: _____  |

Art Unit: 2131

This action is in response to the communication filed on 11/21/2003.

## DETAILED ACTION

Claims 1-47 have been examined.

### *Title*

The title of the invention is acceptable.

### *Information Disclosure Statement*

The information disclosure statement(s) (IDS) submitted on 10/26/2004 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statements.

### *Drawings*

The drawings filed on 5/10/2004 are acceptable for examination proceedings.

### *Specification*

Applicant is reminded of the proper language and format for an abstract of the disclosure.

*The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.*

*The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.*

The abstract of the disclosure is objected to because:

The abstract should be limited to one paragraph.

Correction is required. See MPEP § 608.01(b).

Art Unit: 2131

*Claim Objections*

Claims 1-23, 25-26, 29-31, 35, 37, 39, and 40 are objected to because of the following informalities: All of these claims suffer from at least one of the following informalities:

A. Lack of a terminating period.

B. Use of a comma in place of a terminating period.

C. Lack of antecedent basis for the limitation "the internet". The examiner will assume that the claim language was meant to read "an internet" for purposes of searching prior art.

Claim 25 is not listed in the claim listing, and claim 26 depends from claim 25. The examiner will assume that claim 26 was meant to depend from claim 24.

Claim 39 recites the limitation "hatched string" which the examiner believes was meant to read "hashed string".

In claim 40, the limitation "the strip" lacks antecedent basis in the claim. The examiner will assume for the purposes of searching prior art, that the limitation was meant to read "the string".

The examiner encourages the applicant to carefully review each and every claim to ensure that no other typographical errors have been overlooked.

Appropriate correction is required.

*Duplicate Claims, Warning*

Applicant is advised that should claim 29 be found allowable, claim 32 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing,

Art Unit: 2131

1 despite a slight difference in wording, it is proper after allowing one claim to object to the other  
2 as being a substantial duplicate of the allowed claim. Applicant is required to either cancel or  
3 amend one of the two claims in order to correct this issue. See MPEP § 706.03(k).

4  
5 ***Claim Rejections - 35 USC § 102***

6 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the  
7 basis for the rejections under this section made in this Office action:

8 *A person shall be entitled to a patent unless –*

9 *(b) the invention was patented or described in a printed publication in this or a foreign*  
10 *country or in public use or on sale in this country, more than one year prior to the date of*  
11 *application for patent in the United States.*

12  
13 Claims 1-24, 26-32 and 40-42 are rejected under 35 U.S.C. 102(b) as being anticipated by  
14 Tomkow (WO 01/10090).

15 Regarding claims 1, 8, and 14, Tomkow disclosed a method of transmitting a message  
16 from a sender to a recipient through a server displaced from the recipient (See Tomkow  
17 Abstract), including the steps at the server of: receiving the message at the server from the sender  
18 (See Tomkow Page 29 Lines 16-18), transmitting from the server to the recipient the message  
19 and an attachment including the identity and address of the recipient and the identity of the  
20 sender and the time of the transmittal (See Tomkow Page 30 Line 14 – Page 31 Line 26),  
21 receiving the message and the attachment at the server from the recipient (See Tomkow Page 30  
22 Line 14 – Page 31 Line 26), providing digital signatures of the message and the attachment at the  
23 server (See Tomkow Page 29 Lines 19 – Page 30 Line 11), and authenticating to the recipient the  
24 message and the attachment at the server on the basis of the information received by the recipient

1 from the server and on the basis of the digital signatures provided by the server (See Tomkow  
2 Page 41 Line 28 – Page 42 Line 15).

3       Regarding claims 24, 27, and 33, Tomkow disclosed in a method of transmitting a  
4 message from a sender to a recipient through a server displaced from the recipient (See Tomkow  
5 Abstract), the steps at the server of: receiving the message from the recipient at a web site  
6 providing at the server for an indication of the authenticity of the message (See Tomkow Page 41  
7 Lines 28-32), providing a compressed encrypted version of the message where the compression  
8 is a particular compression and the encryption is a particular encryption (See Tomkow Page 41  
9 Lines 30-32), decompressing the message in accordance with the particular compression to  
10 provide a first digital fingerprint of the message (See Tomkow Page 42 Lines 1-2), decrypting  
11 the compressed encrypted version of the message in accordance with the particular encryption to  
12 provide a second digital fingerprint of the message (See Tomkow Page 41 Lines 30-32), and  
13 comparing the first and second digital fingerprints of the message to determine the authenticity  
14 of the message (See Tomkow Page 42 Lines 2-15).

15       Regarding claim 40, Tomkow disclosed in a method of transmitting a message and an  
16 attachment from a sender through a server displaced from the recipient, the steps at the server of:  
17 identifying the sender (See Tomkow Page 16 Line 10 – Page 17 Line 5), providing the  
18 attachment and the message stripped of the attachment (See Tomkow Page 29 Lines 21-31),  
19 providing a string formed from the identification of the sender, the attachment and the message  
20 stripped of the attachment (See Tomkow Page 40 Lines 19-31), and hashing the string (See  
21 Tomkow Page 40 Lines 19-31).

1           Regarding claim 2, Tomkow disclosed that the server creates digital fingerprints from the  
2 digital signatures and from the message and the attachment to authenticate the message and the  
3 attachment on the basis of the digital fingerprints (See Tomkow Page 12 Lines 1-6 and Page 29  
4 Lines 21-26 and Page 40 Lines 19-31).

5           Regarding claim 3, Tomkow disclosed that the attachment includes interim stations  
6 between the recipient and the server (See Tomkow Page 2 Lines 1-3) and wherein the message  
7 and the attachment, and the digital signatures of the message and the attachment, are transmitted  
8 from the server to the sender to provide for a determination at the server for the sender of the  
9 authenticity of the message and the attachment (See Tomkow Page 22 Line 14 – Page 23 Line  
10 30).

11           Regarding claim 4, Tomkow disclosed that the message and the attachment and the  
12 digital signatures of the message and the attachment are not retained at the sender when the  
13 message and the attachment and the digital signatures are transmitted from the server to the  
14 sender (See Tomkow Page 25 Lines 15-21).

15           Regarding claim 5, Tomkow disclosed that the message and the attachment and the  
16 digital signatures of the message and the attachment are transmitted from the server to the sender  
17 (See Tomkow Page 22 Line 15 – Page 23 Line 30).

18           Regarding claim 6, Tomkow disclosed that the sender transmits to the server, to  
19 authenticate the message, the information supplied by the server to the sender and wherein the  
20 server operates upon the information from the sender to authenticate the message (See Tomkow  
21 Page 26 Line 1 – Page 28 Line 4).

1           Regarding claim 7, Tomkow disclosed that the message and the digital signature of the  
2 message are discarded after the message and the digital signature are transmitted by the server to  
3 the sender (See Tomkow Page 25 Lines 4-16).

4           Regarding claim 9, Tomkow disclosed transmitting to the recipient the state of  
5 authenticity of the message on the basis of the results of the comparison of the digital  
6 fingerprints (See Tomkow Page 41 Line 28 – Page 42 Line 15).

7           Regarding claim 10, Tomkow disclosed transmitting to the server the message and the  
8 attachment, and receiving from the sender the message and the attachment and the digital  
9 signatures of the message and the attachment, producing digital fingerprints of the message, the  
10 attachment and the digital signatures, and comparing the digital fingerprints relating to the  
11 message, and the digital fingerprints relating to the attachment, to determine the authenticity of  
12 the message and the attachment (See Tomkow Page 26 Line 1 – Page 28 Line 4).

13           Regarding claim 11, Tomkow disclosed disposing of the message and the attachment and  
14 the digital signatures of the message and the attachment after transmitting this information to the  
15 sender (See Tomkow Page 25 Lines 4-16).

16           Regarding claim 12, Tomkow disclosed at the server: providing at the server, at the same  
17 time as the reception of the message, an attachment including the identity of the sender and the  
18 identity and address of the server and the identity and address of the recipient and the time of  
19 transmission of the message from the server to the recipient (See Tomkow Page 30 Line 14 –  
20 Page 31 Line 26), transmitting from the server to the recipient the attachment at the same time as  
21 the transmission of the message (See Tomkow Page 30 Line 14 – Page 31 Line 26), and  
22 receiving from the recipient at the server the message and the attachment (See Tomkow Page 30



Art Unit: 2131

1 Line 14 – Page 31 Line 26), providing digital fingerprints of the message, the attachment and the  
2 digital signatures of the message and the attachment (See Tomkow Page 41 Line 28 – Page 42  
3 Line 15), providing an indication of the authentication of the attachment on the basis of a  
4 comparison at the server of the digital fingerprints relating to the message and the digital  
5 fingerprints relating to the attachment (See Tomkow Page 41 Line 28 – Page 42 Line 15).

6 Regarding claim 13, Tomkow disclosed transmitting from the server to the recipient an  
7 indication of the authenticity of the message on the basis of the comparison of the digital  
8 fingerprints relating to the message and the digital fingerprints relating to the attachment (See  
9 Tomkow Page 41 Line 28 – Page 42 Line 15).

10 Regarding claim 15, Tomkow disclosed that digital fingerprints are provided at the server  
11 of the message and the attachment and digital fingerprints are provided at the server of the digital  
12 signatures of the message and the attachment (See Tomkow Page 41 Line 28 – Page 42 Line 15)  
13 and wherein a comparison is provided at the server of the digital fingerprints of the message and  
14 the digital signature of the message, and the attachment and the digital signature of the  
15 attachment, to determine the authenticity of the message and the attachment (See Tomkow Page  
16 41 Line 28 – Page 42 Line 15).

17 Regarding claim 16, Tomkow disclosed that the indications of the state of authenticity of  
18 the message and the attachment are transmitted from the server to the recipient (See Tomkow  
19 Page 41 Line 28 – Page 42 Line 15) and wherein the message and the attachment and the digital  
20 signatures of the message and the attachment are discarded at the server when the indications of  
21 the authenticity of the message and the attachment are transmitted from the server to the  
22 recipient (See Tomkow Page 35 Lines 11-13).

Art Unit: 2131

1           Regarding claim 17, Tomkow disclosed that the message and the attachment and the  
2 digital signatures of the message and the attachment are transmitted from the server to the sender  
3 and wherein the server produces digital fingerprints of the message and the attachment and  
4 digital fingerprints of the digital signature of the message and the attachment and wherein the  
5 server compares the digital fingerprints relating to the message, and the digital fingerprints  
6 relating to the attachment, to determine the authenticity of the message and the attachment (See  
7 Tomkow Page 22 Line 14 – Page 23 Line 30 and Page 26 Line 1 – Page 28 Line 4).

8           Regarding claim 18, Tomkow disclosed that the server transmits to the recipient the  
9 results of the comparison and wherein the server discards the message and the attachment and  
10 the digital signatures of the message and the attachment when the server transmits the message  
11 and the attachment and the digital signature of the message and the attachment to the recipient  
12 (See Tomkow Page 25 Line 3 – Page 28 Line 4).

13           Regarding claim 28, Tomkow disclosed transmitting to the recipient the results of the  
14 comparison of the first and second digital fingerprints of the message and the first and second  
15 digital fingerprints of the attachment (See Tomkow Page 41 Line 28 – Page 42 Line 15).

16           Regarding claims 19-23, 26, 30, 31 Tomkow disclosed that the message is received at the  
17 server through the internet and wherein the message and the digital signature of the message are  
18 transmitted to the recipient through the internet, and that the state of authenticity of the message  
19 is transmitted through the internet to the recipient (See Tomkow Page 43 Lines 3-28).

20           Regarding claims 29 and 32, Tomkow disclosed the attachment includes the identity of  
21 the sender and the identity and the address of the server and the identity and address of the

1 recipient and the time of transmission of the message from the server to the recipient (See  
2 Tomkow Page 30 Line 14 – Page 31 Line 26).

3 Regarding claim 41, Tomkow disclosed hashing the string, and encrypting the hash of the  
4 hashed string (See Tomkow Page 41 Lines 19-27).

5 Regarding claim 42, Tomkow disclosed digitally sealing the encrypted hash of the hashed  
6 string, attaching the message to the encrypted hash of the hashed string, and sending to the  
7 recipient the message and the encrypted hash of the hashed string (See Tomkow Page 41 Lines  
8 19-27).

9  
10 ***Claim Rejections - 35 USC § 103***

11 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all  
12 obviousness rejections set forth in this Office action:

13 *A patent may not be obtained though the invention is not identically disclosed or*  
14 *described as set forth in section 102 of this title, if the differences between the subject matter*  
15 *sought to be patented and the prior art are such that the subject matter as a whole would have*  
16 *been obvious at the time the invention was made to a person having ordinary skill in the art to*  
17 *which said subject matter pertains. Patentability shall not be negated by the manner in which*  
18 *the invention was made.*  
19

20 Claims 33-37, and 43-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over  
21 Tomkow as applied to claim 1 above, and further in view of Stark et al (Patent Application  
22 Publication 2002/0131566) hereinafter referred to as Stark.

23 Regarding claim 33, Tomkow disclosed an a method of transmitting a message from a  
24 sender through a server displaced from the recipient, the steps at the server of: receiving the  
25 message and an attachment from the recipient at a website providing at the server for an

Art Unit: 2131

1 indication of the authenticity of the message (See Tomkow Page 41 Lines 28-32), providing at  
2 the server for an encrypted version of the combination of the message and the attachment (See  
3 Tomkow Page 41 Lines 19-32), decrypting the encrypted version of the combination of the  
4 message and the attachment in accordance with the particular encryption to provide a digital  
5 fingerprint of the combination of the message and the attachment (See Tomkow Page 41 Lines  
6 32-33), and comparing second digital fingerprint to determine the authenticity of the message  
7 and the attachment (See Tomkow Page 42 Lines 1-5), but Tomkow failed to disclose that the  
8 encrypted version was also compressed, decompressing the compressed encrypted version of the  
9 combination of the message and the attachment in accordance with the particular compression to  
10 provide a first digital fingerprint of the combination of the message and the attachment for  
11 comparison.

12 Stark teaches that in order to make email data smaller, the data should be compressed to  
13 make it smaller prior to transmission, and should be decompressed upon reception (See Stark  
14 Abstract).

15 It would have been obvious to the ordinary person skilled in the art at the time of  
16 invention to employ the teachings of Stark in the email system of Tomkow by compressing the  
17 modified message, and later decompressing the modified message in order to allow for  
18 comparison. This would have been obvious because the ordinary person skilled in the art at the  
19 time of invention would have been motivated to provide a smaller message for transmission.

20 Regarding claim 43, Tomkow disclosed in a method of authenticating at a recipient a  
21 message and an attachment transmitted from a sender to the recipient through a server displaced  
22 from the recipient, the steps of: providing at the recipient a string comprising an encrypted

Art Unit: 2131

1 embedded hash of a string including an identification of the sender, the message and a hash of  
2 the attachment (See Tomkow Page 41 Lines 19-32), decrypting the string (See Tomkow Page 41  
3 Lines 32-33), hashing the string less the hash of the string (See Tomkow Page 42 Line 1),  
4 comparing the hash produced in the string and the embedded hash (See Tomkow Page 42 Lines  
5 1-2), and using the results of the comparison to indicate to the recipient the authenticity of the  
6 message and the attachment (See Tomkow Page 42 Lines 2-15), but Tomkow failed to disclose  
7 that the encrypted string was compressed, or decompressing the encrypted string.

8 Stark teaches that in order to make email data smaller, the data should be compressed to  
9 make it smaller prior to transmission, and should be decompressed upon reception (See Stark  
10 Abstract).

11 It would have been obvious to the ordinary person skilled in the art at the time of  
12 invention to employ the teachings of Stark in the email system of Tomkow by compressing the  
13 modified message, and later decompressing the modified message in order to allow for  
14 comparison. This would have been obvious because the ordinary person skilled in the art at the  
15 time of invention would have been motivated to provide a smaller message for transmission.

16 Regarding claim 46, Tomkow disclosed in a method of authenticating at a recipient a  
17 message and an attachment transmitted from a sender to the recipient, providing an attachment  
18 (See Tomkow Page 41 Lines 19-32), providing at the recipient on encryption of a hashed string  
19 including information relating to the identification of the sender, the attachment and the message  
20 stripped of the attachment (See Tomkow Page 41 Lines 19-32), decrypting the encrypted hash of  
21 the hashed string (See Tomkow Page 41 Lines 32-33), separating the hash from the string (See  
22 Tomkow Page 42 Line 1), forming a hash from the information relating to the identification of

1 the sender, the attachment and the message stripped of the attachment (See Tomkow Page 42  
2 Lines 1-2), comparing the hash separated from the string and the hash formed from the  
3 information in the string (See Tomkow Page 42 Lines 2-15), and using the results of the  
4 comparison to indicate to the recipient the authenticity of the message and the attachment (See  
5 Tomkow Page 42 Lines 2-15), but Tomkow failed to disclose that the encrypted string was  
6 compressed, or decompressing the encrypted string.

7 Stark teaches that in order to make email data smaller, the data should be compressed to  
8 make it smaller prior to transmission, and should be decompressed upon reception (See Stark  
9 Abstract).

10 It would have been obvious to the ordinary person skilled in the art at the time of  
11 invention to employ the teachings of Stark in the email system of Tomkow by compressing the  
12 modified message, and later decompressing the modified message in order to allow for  
13 comparison. This would have been obvious because the ordinary person skilled in the art at the  
14 time of invention would have been motivated to provide a smaller message for transmission.

15 Regarding claim 34, the combination of Tomkow and Stark disclosed transmitting to the  
16 recipient the results of the comparison of the first and second digital fingerprints (See Tomkow  
17 Page 41 Line 28 – Page 42 Line 15).

18 Regarding claim 35, see the rejection of claim 19 above.

19 Regarding claims 36 and 37, see the rejection of claim 29 above.

20 Regarding claims 44 and 47, Tomkow and Stark disclosed separating the attachment  
21 from the message, hashing the separated attachment, comparing the hashed separated attachment  
22 and the hashed attachment in the string, and using the results of the comparison provided in the

1 previous step to indicate the authenticity of the message and the attachment (See Tomkow Page  
2 41 Line 19 – Page 42 Line 15).

3 Regarding claim 45, Tomkow and Stark disclosed recovering the message and the  
4 attachment and transmitting the recovered message and attachment to the recipient with the  
5 indication of their authenticity (See Tomkow Page 41 Lines 19-25).

6 Claims 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tomkow as  
7 applied to claim 1 above, and further in view of Kaufman et al. (US Patent Number 5,764,772)  
8 hereinafter referred to as Kaufman.

9 Regarding claim 38, Tomkow disclosed in a method of transmitting a message and an  
10 attachment from a sender to a recipient through a server displaced from the recipient, including  
11 the steps at the server of identifying the sender (See Tomkow Page 40 Lines 19-24), hashing the  
12 attachments (See Tomkow Page 40 Lines 21-25), stripping the message of the attachments,  
13 hashing the identification of the sender, the hashed attachments and the message to form a  
14 hashed string (See Tomkow Page 40 Lines 22-26), encrypting the hashed string (See Tomkow  
15 Page 40 Lines 26-28), and digitally sealing the encrypted hash of the hashed string (See Tomkow  
16 Page 40 Lines 26-30), but Tomkow failed to disclose hashing the hashed string and encrypting  
17 the result if the hashing of the hashed string.

18 Kaufman teaches that in order to protect against the use of a lookup table to compute  
19 hashes, the hash should be performed multiple times (See Kaufman Col. 10 Line 64-Col. 11  
20 Line 6).

21 It would have been obvious to the ordinary person skilled in the art at the time of  
22 invention to employ the teachings of Kaufman by hashing the hashes of Tomkow. This would

Art Unit: 2131

1 have been obvious because the ordinary person skilled in the art would have been motivated to  
2 prevent the generation of a hash table corresponding to the hashing system.

3 Regarding claim 39, Tomkow and Kaufman disclosed adding the message to the  
4 encrypted hash of the hashed string, and transmitting the message and the encrypted hash of the  
5 hashed string to the recipient (See Tomkow Page 40 Lines 26-31).

6 *Conclusion*

7 Claims 1-24, and 26-47 have been rejected, and claim 25 is objected to as not being  
8 listed.

9 The prior art made of record and not relied upon is considered pertinent to applicant's  
10 disclosure.

11 Any inquiry concerning this communication or earlier communications from the  
12 examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.  
13 The examiner can normally be reached on M-F 8-4.

14 If attempts to reach the examiner by telephone are unsuccessful, the examiner's  
15 supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the  
16 organization where this application or proceeding is assigned is 571-273-8300.



Art Unit: 2131

1 Information regarding the status of an application may be obtained from the Patent  
2 Application Information Retrieval (PAIR) system. Status information for published applications  
3 may be obtained from either Private PAIR or Public PAIR. Status information for unpublished  
4 applications is available through Private PAIR only. For more information about the PAIR  
5 system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR  
6 system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would  
7 like assistance from a USPTO Customer Service Representative or access to the automated  
8 information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

9  
10  
11  
12 /Matthew Henning/  
13 Assistant Examiner  
14 Art Unit 2131  
15 7/6/2007

  
SYED A. ZIA 12/19/2007  
PRIMARY EXAMINER